WHAT IS CLAIMED IS:

1. An electronic seal, comprising:

an input section for inputting a random number encrypted based on a prescribed key;

a secret key memory section for storing a secret key related to the prescribed key;

a decoding section for decoding the input random number based on the secret key;

an encryption section for encrypting the decoded random number based on the secret key; and

an output section for outputting the random number encrypted based on the secret key.

2. An electronic seal according to claim 1, wherein:

when the input section inputs a first response request ID encrypted based on the prescribed key, the decoding section decodes the input first response request ID based on the secret key,

the electronic seal further includes a response request ID memory section for storing a second response request ID, and a comparison section for comparing the decoded first response request ID and the second response request ID, and

when the decoded first response request ID matches the second response request ID, the encryption section encrypts the decoded random number.

3. An electronic seal according to claim 1, wherein:

the secret key memory section stores a plurality of secret keys respectively corresponding to a plurality of card company ID numbers, and

when the input section inputs a card company ID number, the secret key memory section specifies the secret key corresponding to the input card company ID number among the plurality of secret keys.

4. An electronic seal according to claim 1, wherein the prescribed key is a public key, and the secret key and the public key form a key pair via a prescribed function.

5. A mobile device including an electronic seal according to claim 1.

6. An IC card, comprising:

a random number generation section for generating a random number;

a prescribed key memory section for storing a

prescribed key;

an encryption section for encrypting the generated random number based on the prescribed key;

an output section for outputting the random number encrypted based on the prescribed key;

an input section for inputting a random number encrypted based on a secret key related to the prescribed key;

a decoding section for decoding the input random number based on the prescribed key; and

a comparison section for comparing the random number generated by the random number generation section and the decoded random number.

7. An IC card according to claim 6, further comprising an authentication section for, when the random number generated by the random number generation section matches the decoded random number, authenticating the user; and when the random number generated by the random number generation section does not match the decoded random number, rejecting the user.

8. An IC card according to claim 6, further comprising a response request ID memory section for storing a response

request ID, wherein:

the encryption section encrypts the response request ID based on the prescribed key, and

the output section outputs the encrypted response request ID.

9. An IC card according to claim 6, further comprising a card company ID number memory section for storing a card company ID number, wherein the output section outputs the card company ID number.

10. An IC card according to claim 6, wherein the prescribed key memory section stores a plurality of prescribed keys respectively corresponding to a plurality of card company ID numbers.

11. An IC card according to claim 6, wherein the prescribed key is a public key, and the secret key and the public key form a key pair via a prescribed function.

12. An authentication system comprising:

an IC card, and

an electronic seal,

wherein:

the IC card includes:

a random number generation section for generating a random number,

a prescribed key memory section for storing a prescribed key,

a first encryption section for encrypting the generated random number based on the prescribed key, and

a first output section for outputting the random number encrypted based on the prescribed key;

the electronic seal includes:

a second input section for inputting the random number encrypted based on the prescribed key,

a secret key memory section for storing a secret key related to the prescribed key,

a second decoding section for decoding, based on the secret key, the random number encrypted based on the prescribed key,

a second encryption section for encrypting, based on the secret key, the random number decoded based on the secret key, and

a second output section for outputting the random number encrypted based on the secret key;

the IC card further includes:

a first input section for inputting the random

number encrypted based on the secret key,

a first decoding section for decoding, based on the prescribed key, the random number encrypted based on the secret key, and

a comparison section for comparing the random number generated by the random number generation section and the random number decoded based on the prescribed key; and

the IC card and the electronic seal mutually exchange data for performing authentication.

13. An authentication system according to claim 12, wherein the IC card further includes an authentication section for, when the random number generated by the random number generation section matches the random number decoded based on the prescribed key, authenticating the user; and when the random number generated by the random number generation section does not match the random number decoded based on the prescribed key, rejecting the user.

14. An authentication system according to claim 12, wherein the prescribed key is a public key, and the secret key and the public key form a key pair via a prescribed function.

15. An electronic seal, comprising:

an input section for inputting a random number encrypted based on a prescribed key;

a secret key memory section for storing a secret key related to the prescribed key;

a decoding section for decoding the input random number based on the secret key;

a user's inherent information memory section for storing a user's inherent information;

a hash operation section for performing a hash operation using the decoded random number and the user's inherent information so as to output a hash operation result;

an encryption section for encrypting the hash operation result based on the secret key; and

an output section for outputting the encrypted hash operation result.

16. An electronic seal according to claim 15, wherein:

when the input section inputs a first response request ID encrypted based on the prescribed key, the decoding section decodes the input first response request ID based on the secret key,

the electronic seal further includes a response request ID memory section for storing a second response request ID, and a comparison section for comparing the decoded first response request ID and the second response request ID, and

when the decoded first response request ID matches the second response request ID, the encryption section encrypts the hash operation result.

17. An electronic seal according to claim 15, wherein:

the secret key memory section stores a plurality of secret keys respectively corresponding to a plurality of card company ID numbers, and

when the input section inputs a card company ID number, the secret key memory section specifies the secret key corresponding to the input card company ID number among the plurality of secret keys.

18. An electronic seal according to claim 15, wherein the prescribed key is a public key, and the secret key and the public key form a key pair via a prescribed function.

19. A mobile device including an electronic seal according to claim 15.

20. An IC card, comprising:

a random number generation section for generating a random number;

a prescribed key memory section for storing a prescribed key;

an encryption section for encrypting the generated random number based on the prescribed key;

an output section for outputting the encrypted random number;

a user's inherent information memory section for storing user's inherent information;

a hash operation section for performing a hash operation using the generated random number and the user's inherent information so as to output a first hash operation result;

an input section for inputting a second hash operation result encrypted based on a secret key related to the prescribed key;

a decoding section for decoding the input second hash operation result based on the prescribed key; and

a comparison section for comparing the first hash operation result output from the hash operation section and the decoded second hash operation result.

21. An IC card according to claim 20, further comprising an authentication section for, when the first hash operation result output from the hash operation section matches the decoded second hash operation result, authenticating the user; and when the first hash operation result output from the hash operation section does not match the decoded second hash operation result, rejecting the user.

22. An IC card according to claim 20, further comprising a response request ID memory section for storing a response request ID, wherein:

the encryption section encrypts the response request ID based on the prescribed key, and

the output section outputs the encrypted response request ID.

23. An IC card according to claim 20, further comprising a card company ID number memory section for storing a card company ID number, wherein the output section outputs the card company ID number.

24. An IC card according to claim 20, wherein the prescribed

key memory section stores a plurality of prescribed keys respectively corresponding to a plurality of card company ID numbers.

25. An IC card according to claim 20, wherein the prescribed key is a public key, and the secret key and the public key form a key pair via a prescribed function.

26. An authentication system comprising:

an IC card, and

an electronic seal,

wherein:

the IC card includes:

a random number generation section for generating a random number,

a prescribed key memory section for storing a prescribed key,

a first encryption section for encrypting the generated random number based on the prescribed key,

a first output section for outputting the encrypted random number,

a first user's inherent information memory section for storing a user's inherent information, and

a first hash operation section for performing a

hash operation using the user's inherent information stored in the first user's inherent information memory section and the generated random number so as to output a first hash operation result;

the electronic seal includes:

a second input section for inputting the encrypted random number,

a secret key memory section for storing a secret key related to the prescribed key,

a second decoding section for decoding, based on the secret key, the encrypted random number,

a second user's inherent information memory section for storing user's inherent information,

a second hash operation section for performing a hash operation using the user's inherent information stored in the second user's inherent information memory section and the decoded random number so as to output a second hash operation result,

a second encryption section for encrypting the second hash operation result based on the secret key, and

a second output section for outputting the encrypted second hash operation result;

the IC card further includes:

a first input section for inputting the encrypted

second hash operation result,

a first decoding section for decoding, based on the prescribed key, the encrypted second hash operation result,

a comparison section for comparing the first hash operation result and the decoded second hash operation result; and

the IC card and the electronic seal mutually exchange data for performing authentication.

27. An authentication system according to claim 26, wherein the IC card further includes an authentication section for, when the first hash operation result matches the decoded second hash operation result, authenticating the user; and when the first hash operation result does not match the decoded second hash operation result, rejecting the user.

28. An authentication system according to claim 26, wherein the prescribed key is a public key, and the secret key and the public key form a key pair via a prescribed function.